DEPARTMI

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of modified system of records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs is amending the system of records currently entitled "Health Program Evaluation—VA" (107VA008B) as set forth in the *Federal Register*. VA is amending the system by updating Routine Uses of Records Maintained in the System, Safeguards, Retention and Disposal, and System Manager and Address as well as Notification Procedure. VA is republishing the system notice in its entirety.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the *Federal Register*. If no public comment is received during the period allowed for comment or unless otherwise published in the *Federal Register* by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the *Federal Register*. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Written comments may be submitted through www.Regulations.gov; by mail or hand-delivery to Director, Regulation Policy and Management (00REG), Department of Veterans Affairs, 810 Vermont Ave. NW, Room 1064, Washington, DC 20420; or by fax to (202) 273-9026 (not a toll-free number). Comments should indicate that they are submitted in response to Health Program Evaluation—VA (107VA008B). Copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461-4902 for an

appointment. (This is not a toll-free number.) In addition, comments may be viewed online at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: Office of Enterprise Integration (OEI), Ryan J. Stiegman, Privacy Officer, U.S. Department of Veterans Affairs, 810 Vermont Ave., NW., Washington, DC 20420; telephone (202) 461-5800.

SUPPLEMENTARY INFORMATION:

Health Program Evaluation—VA (107VA008B) has been amended to reflect the current organizational alignment; new mail addresses, and updated point of contact information. The Department has also made minor edits to the System Notice for clarity, completeness, grammar, and to reflect plain language.

The System Location Section has been amended to provide an update to the name of VA's Austin Information Technology Center at 1615 Woodward St., Austin, TX 78772.

The System Manager, Notification Procedure, Record Access Procedure and Contesting Record Procedures name and address information have been changed to reflect new organizational alignments. The System Manager is Executive Director, Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420. Finally, the Report of Intent to Publish has been amended to include a link to a more complete description of the duties and activities of the Office of Enterprise Integration at http://www.va.gov/OP3.

Minor changes to Routine Use language have been done in updating language to use VA's library of approved VA routine uses. Changes to improve clarity or organizational address information include the following Routine Uses.

Routine Use One (1) has been amended for clarification to "VA may disclose information from the record of an individual in response to an inquiry from the congressional office made at the request of that individual." VA must be able to provide

information about individuals to adequately respond to inquiries from Members of Congress at the request of constituents who have sought their assistance.

Routine Use Two (2) has been amended to use current updated language for National Archives and Record Administration (NARA) and General Services Administration (GSA) that reads “VA may disclose information from this system to the National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under title 44, U.S.C.” NARA is responsible for archiving old records which are no longer actively used but may be appropriate for preservation, and for the physical maintenance of the Federal government’s records. VA must be able to provide the records to NARA in order to determine the proper disposition of such records.

Routine Use Four (4) has been amended to use current VA update language for this use. This language states “VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement.”

“This routine use includes disclosures by an individual or entity performing services for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.”

This routine use, which also applies to agreements that do not qualify as contracts defined by Federal procurement laws and regulations, is consistent with OMB guidance in OMB Circular A-130, App. I, paragraph 5a (1) (b) that agencies promulgate

routine uses to address disclosure of Privacy Act-protected information to contractors in order to perform the services contracts for the agency.

Routine Use Six (6) has been amended to use the current VA update language for this particular use. This amendment reads “VA may, on its own initiative, disclose information from this system to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.”

This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724.

a. Effective Response. A federal agency’s ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions. In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. 552a (b) (3) of the Privacy Act, agencies should publish a routine use for appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach.

Routine Use Seven (7) providing current posting location of “Privacy Act Guidance – Update” has been amended to http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

The notice of intent to publish and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Routine Use Eight (8) VA may, on its own initiative, disclose information in this system, except the names and home addresses of veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, state, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. On its own initiative, VA may also disclose the names and addresses of veterans and their dependents to a Federal agency charged with the responsibility of

investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

VA must be able to provide on its own initiative information that pertains to a violation of laws to law enforcement authorities in order for them to investigate and enforce those laws. Under 38 U.S.C. 5701(a) and (f), VA may only disclose the names and addresses of veterans and their dependents to Federal entities with law enforcement responsibilities. This is distinct from the authority to disclose records in response to a qualifying request from a law enforcement entity, as authorized by Privacy Act subsection 5 U.S.C. 552a(b)(7).

The Report of Intent to Amend a System of Records Notice and an advance copy of the system notice have been sent to the appropriate congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. James P. Gfrerer, Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on April 17, 2020 for publication.

Dated: January 19, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

107VA008B

SYSTEM NAME: Health Program Evaluation—VA

SYSTEM LOCATION:

Electronic records are located on the Department of Veterans Affairs' (VA's) secured servers housed at VA's Austin Information Technology Center, 1615 Woodward St., Austin, TX, 78772. Records necessary for a contractor to perform under a VA-approved contract are located at the respective contractor's facility.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Authority to maintain this system of Record is contained in Title 38, U.S.C 527.

PURPOSE(S): For the conduct of health-related qualitative, quantitative, and actuarial analyses and projections to support policy analyses and recommendations for improving VA services for Veterans and their families. Analysis and review of health data, policy and planning issues affecting Veterans programs to support legislative, regulatory, policy recommendations and initiatives.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Veterans who have applied for healthcare services or benefits under 38 U.S.C.
2. Veterans' spouse, surviving spouse, previous spouse, children, and parents who have applied for healthcare services or benefits under 38 U.S.C.
3. Beneficiaries of other Federal agencies or other governmental entities.
4. Individuals examined or treated under contract or resource sharing agreements.
5. Individuals examined or treated for research or donor purposes.
6. Individuals who have applied for 38 U.S.C. benefits but who do not meet the requirements under 38 U.S.C. to receive such benefits.
7. Individuals who were provided medical care under emergency conditions for humanitarian reasons.
8. Pensioned members of allied forces provided healthcare services under 38 U.S.C.

CATEGORIES OF RECORDS IN THE SYSTEM: Records include identification numbers, contact and location information, demographic information, military service descriptions, residency characteristics, economic information, healthcare visit descriptions, patient assessments, medical test descriptions and results, diagnoses, disability assessments, treatments, pharmaceutical information, service utilization and associated medical staffing and resource costs, entitlements or benefits, patient survey results, and health status. The records include information created or collected during the course of normal clinical operations work and is provided by patients, employers, students, volunteers, contractors, subcontractors, and consultants. In addition, records also include social security numbers, military service numbers, claim or file numbers, and DoD's identification numbers.

RECORD SOURCE CATEGORIES: Information is obtained from VHA and other VA staff offices and Administrations, OPP's National Survey of Veterans, national survey's (e.g. National Long-Term Care Survey, National Health Interview Survey), Federal Agencies (e.g. Department of Defense, Department of Health and Human Services), state agencies, and other private and public health provider data sources or insurance programs and plans.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To the extent that records contained in the system include information protected by 45 CFR Parts 160 and 164, i.e., individually identifiable health information, and 38 U.S.C. 7332, i.e., medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia, or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR Parts 160 and 164 permitting disclosure.

1. The record of an individual who is covered by a system of records may be disclosed to a Member of Congress or a staff person acting for the Member, when the Member or staff person requests the record on behalf of and at the written request of the individual.

2. VA may disclose information from this system to the National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under title 44, U.S.C.

3. Any system records may be disclosed to a Federal agency for the conduct of research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency, provided that there is legal authority under all applicable confidentiality statutes and regulations to provide the data and OEI has determined prior to the disclosure that OEI data handling requirements are satisfied. OEI may disclose limited individual identification information to another Federal agency for the purpose of matching and acquiring information held by that agency for OEI to use for the purposes stated for this system of records.

4. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement.

5. Any system records may be disclosed to the Office of Management and Budget in order for them to perform their statutory responsibilities of evaluating Federal programs.

6. VA may, on its own initiative, disclose information from this system to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise

there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

7. VA may disclose information in this system of records to the Department of Justice (DOJ), either on VA's initiative or in response to DOJ's request for the information, after either VA or DOJ determines that such information is relevant to DOJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that disclosure of the records to DOJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. In determining whether to disclose records under this routine use, VA will comply with the guidance promulgated by the Office of Management and Budget in a May 24, 1985, memorandum entitled "Privacy Act Guidance - Update", currently posted at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

8. VA may disclose on its own initiative any information in this system, except the names and home addresses of Veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory

in nature, and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, state, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. On its own initiative, VA may also disclose the names and addresses of Veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

VA sensitive information, including individually identifiable health information, is stored on a segregated secure server. Data stored on secure servers are located at the Austin Information Technology Center (AITC). Databases are temporarily placed on a secured server inside a restricted network area for data match purposes only. Information that resides on a segregated server is kept behind locked doors with limited access. Requestors of OEI stored health information within VA, or from external individuals, contractors, organizations, and/or agencies with whom VA has a contract or agreement, must provide an equivalent level of security protection and comply with all applicable VA policies and procedures for storage and transmission as codified in VA directives such as but not limited to *VA Handbook 6500*.

POLICIES AND PRACTICES FOR RETRIEVABILITY OF RECORDS:

Individually-identified health care information is kept in two forms. The first form is the original data file containing the names and social security numbers of the record subjects. OEI assigns unique codes derived from social security numbers to these individual records prior to conducting analyses on the data. The original records may be retrieved using social security number, military service number, claim or file number,

DoD identification number, or other personal numerical identifiers. The records containing the encrypted identifiers may be retrieved only by those identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Electronic records are archived to provide verification of analysis and to provide data for identifying trends that effect veteran beneficiaries and their VA programs. Destruction of any sensitive Personally Identifiable Information (PII) or Protected Health Information (PHI) data is done by deleting information on OIT national data support servers. OEI no longer stores paper beneficiary records in its facilities. Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. OEI will publish an amendment to this notice upon issuance of NARA-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OEI destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with Title 36 Code of Federal Regulations (CFR), Section 1234.34, Destruction of Electronic Records, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.”

PHYSICAL, PROCEDURAL AND ADMINISTRATIVE SAFEGUARDS:

This list of safeguards furnished in this System of Record is a general statement of measures taken to protect health information. For example, Health Insurance Portability and Accountability Act (HIPAA) guidelines for protecting health information will be

followed and OEI will adopt evolving health care industry best practices in order to provide adequate safeguards. Further, VA policy directives that specify the standards that will be applied to protect record level information will be provided to VA staff and contractors through mandatory data privacy and security training.

Access to data storage areas is restricted to authorized VA employee or contract staff who has been cleared to work by the VA Office of Operations, Security, and Preparedness. Health information file areas are locked after normal duty hours. VA facilities are protected from outside access by the Federal Protective Service and/or other security personnel.

Access to health information provided by the Veterans Health Administration (VHA) pursuant to a Business Associate Agreement (BAA) is restricted to those OEI employees and contractors who have a need for the information in the performance of their official duties related to the terms of the BAA. As a general rule, full sets of health care information are not provided for use unless authorized by the System Manager the Executive Director for OEI Data Governance and Analysis (DG&A). File extracts provided for specific official uses will be limited to the minimum necessary amount and contain only the information fields needed for the analysis. Data used for analyses will have individual identifying characteristics removed whenever possible.

Security complies with applicable Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). Health information files containing unique identifiers such as social security numbers are encrypted to NIST-verified FIPS 140-2 standard or higher for storage, transport, or transmission. The primary site for data analysis, storage and transfer is located on a segregated server at the Austin Information Technology Center. All files containing PII in transit or at rest are encrypted. Files are kept encrypted at all times except when data

is in immediate use, per specifications by VA Office of Information Technology. NIST publications were consulted in development of security for this system of records.

Contractors and their subcontractors are required to maintain the same level of security as VA staff for health care information that has been disclosed to them. Any data disclosed to a contractor or subcontractor to perform authorized analyses requires the use of Data Use Agreements, Non-Disclosure Statements and Business Associates Agreements to protect health information. Unless explicitly authorized in writing by the VA, sensitive or protected data made available to the contractor and subcontractors shall not be divulged or made known in any manner to any other person. Other federal or state agencies requesting health care information need to execute Data Use Agreements to protect data.

SYSTEM MANAGER(S) AND ADDRESS (ES):

OEI's System Manager is Kshemendra Paul, Executive Director, Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420, 202-461-1052, Kshemendra.Paul@va.gov.

RECORD ACCESS PROCDEURE: An individual (or duly authorized representative of such individual) who seeks access to or wishes to contest records maintained under his or her name or other personal identifier may write, call or visit the individuals listed under Notification Procedure below.

CONTESTING RECORD PROCEDURES: (See Record Access Procedures above.)

NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request to the System Manager, Executive Director, Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420. Such requests must contain a reasonable description of the

records requested. All inquiries must reasonably identify the health care information involved and the approximate date that medical care was provided. Inquiries should include the patient's full name, social security number, telephone number and return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

[FR Doc. 2021-01542 Filed: 1/22/2021 8:45 am; Publication Date: 1/25/2021]